Providing Trust Based Key Exchange Security Approach for Intrusion Detection Using Recommendation Metrics over Manet (Skite) Stv

S. Saravanan, R. Chandrasekaran, Tamil Nadu

A B S T R A C T
Establishing trust relationship among MANET nodes to secure a session is highly demandable research work. SKITE discusses about recommendation trust values which supports variable trust relations among different members engaged in session. SKITE defines and implements variable trust among member nodes and session established based on neighbor node’s recommendation. SKITE has been implemented over AODV protocol which has been compared with existing PROFIDES and SAR schemes. The performance shows that SKITE performs well on test approaches for session maintenance for average sessions maintained over time, and observed average latency observed for packet dropping attack, black hole attack. SKITE performance is well acclaimed for supporting multiple secured sessions in use than other traditional approaches.

INTRODUCTION

Providing an adaptive security (Garg, 2010) to guard against Intrusion by attackers over a communication channel is a long debatable question by researchers. MANET nodes in network are always susceptible to intruder attack, when the intruder nodes are unknown or new to the domain, supporting with variable pair-wise trust values to nodes under mobility need to support in design and implementation challenges. Few security challenges include random node mobility and dynamic algorithmic update, variable service in use, lack of centralized server, open medium and lack of control over traffic intensity due to node update. Any node or network system should adopt to security policies (Cho, 2008; Wang Cheng-Hua, 2012) such as Confidentiality, Authentication, Integrity and Non-repudiation issues. Any threat or vulnerability to system can be understood as violation to confidentiality or missing object integrity due to missing security features.

A MANET node has several physical vulnerabilities (Jin-Hee Cho, 2011). It is lightweight in order to provide mobility and thus can be easily captured or tampered with. Such issues permit a MANET node as a prey to Denial of Service (DoS) attacks designed to diminish its service and bring down its computational capability. The design properties of MANET network is "highly" on mobility and transient with frequent changes in topology. This issue lacks in central control and depends upon cooperation between nodes. These characteristics invite “man in the middle” or usurpation attacks where an untrusted node or system impersonates as a trusted node. A mobile node attacker may seek out another MANET node and adds up to vulnerability issues. The nature of wireless medium and phenomenon of transmission provide high chances of being intercepted leading to attacks. Passive attacks can occur from an eavesdropper who can decipher and compromise the transmitted information. Active attack (Jin-Hee Cho, 2011) leads to an impersonator or usurper to disrupt packet routing by sending misleading control information. Issues of Packet drop attacks (Ukey, 2010) and black Hole attacks (Mishra, 2004) can be considered as active attacks. This approach leads to the attacker to create routes which does not exist and overflow the routing tables. Service may be denied by unnecessarily forwarding packets or requesting services.

SKITE incorporates providing trust value by using pair wise shared secret key along with trust based secured session management such that node with higher trust value can communicate only with node of equivalent of higher trust value and not with a node of lower trust value. This approach suggests an effective
and adaptive trust provisioning such that security is guaranteed for each session. Enabling trust value STv embedded within each mobile node in adhoc network supports in establishing the secured session dependable on the variable service.

The mechanism of node trustworthiness without the help of any central controller or authorities helps to build an independent trust environment. Such mechanisms permit the node to evaluate trustworthiness of other nodes, which helps in malicious node detection, as well improves the network performance. Creating the hypothesis that nodes with the high trust value will give honest recommendations is agreeable on the suggestion that the recommended trust value of node is highly agreeable. SKITE adopts variable trust value assignment, where nodes only of equitable or related recommendation can exchange keys for providing security.

This paper deals with providing trust analysis for MANET nodes involved in communication. Each node involved in communication is considered to be secured node, if it possess a Secured Trust Value key (STv). The node ‘ni’ is valid to hold the key, for a variable time to be alive ‘ta’ seconds. If node is not secured, or if it does not possess the key then the node ‘ni’ is said to be invalid for participation in establishment of communication path. The feature of supporting pairwise key exchange is always an added advantage for handling security breach. The testbed is simulated using ns2 (Network Simulator, 1989), which highly suits to simulate large networks and provides trust methods to be implemented.

The paper is organized as Sections, where Section-1 introduces MANET, its need for trust security and possibilities of attacks. Section-2 discusses on the trust related work and identifies the gaps in research. Section-3 explains the SKITE architecture and functionality along with required definitions and algorithm. Section-4 discusses on the experimental testbed adopted and SKITE’s performance analysis. Section-5 summarizes the work with need for future work.

Related work:

Pair wise key generation and management approaches among mobile member nodes help to support and establish an adaptive trust relation, which supports various services on dynamic mobility. Dynamic peer nodes or groups can establish initial key agreement (IKA) [2] and related Auxiliary update Key Agreement (AKA) operations such as node mobility related to member addition, member deletion, and other internal group functions. Various approaches had been surveyed and analyzed to understand the need for security based trust approaches and key exchange methods.

Various research efforts on providing security were developed for MANETs, which focus on cluster-based IDS for scalability. In such approaches cluster heads lead to single point of failure. The main idea behind cluster-based IDS is that instead of performing host-based IDS at each node, a Cluster Head (CH) is selected to collect security-related information from nodes in a cluster and determines if intrusion has occurred.

Hierarchy Key Trust approach (Jin-Hee Cho, 2011) proposes mechanism to balance security and efficiency, which makes use of two-level Hybrid Key Tree (HKT) based on clusters. In HKT, nodes are organized into clusters whose sizes are adjusted depending on the level of collusion resistance. Cluster management is a major issue in HKT which adds to much delay and cost involved for providing security. Jin-Hee Cho, Ing-Ray Chen adopts a hierarchical key management structure for energy-aware secure multicast group communication in MANETs based on geographic routing. A fixed cluster size without identifying the optimal cluster size to maximize system performance is assumed in this work.

In (Balasubramanian, 2005; Constantinescu, 2010; Stevens, 2004; Xiaoqi, 2004) the optimal cluster or group size to minimize rekeying cost was studied. The analysis, however, is not for mission-oriented GCSs in MANETs. A region-based group key management protocol (Balasubramanian, 2005) to improve the system performance for group key generation and distribution for GCSs in MANETs is considered. The protocol is found to break the operational area into regions to reduce the group key management overhead and supports in providing the protocol scalable to a large number of nodes in a group.

PROFiDES, a concrete protocol (Ravi, 2008) is based on multi-party extension of the well known Diffie-Hellman key exchange protocol works on profile based trust mechanism to provide security among mobile nodes. Sultan (Sultan, 2013) works on a control based authenticated broadcast channel model by the honest participant under the assumption of variant Diffie-Hellman problem. Zhan (Zhan, 2010) has proposed a novel fault-tolerant conference key agreement protocol, in which, each conference only needs to send one message to a semi-trusted node. Upon acceptance the other trusted nodes can participate in the session. The mobility pattern and traffic patterns were generated successfully so that nodes can transmit packets. The malicious nodes were introduced in the network using packet dropping and black hole attack.

Yong (Yong, 2007) and Xiaoqi (2004) operations like packet forwarding, routing, network management, communication, etc between mobile nodes. This paper had carried out a differential study on various kinds of key management schemes with their special features. The trust models (Stevens, 2004) suggested by Stevens et al and routing protocol work to achieve security with support over confidentiality, integrity and availability in mobile ad-hoc networks to gain the secure environment. Group key management suggested by Pathan (2010)
and Mishra (2004) is one of the basic building blocks in collaborative and group-oriented applications in mobile AdHoc Networks (MANETs) (Gong, 2010).

Group key established involves creating and distributing a common secret for all group members. Ben-Jye Chang et al (2009) proposed, simple and efficient group key (SEGK) management scheme for MANETs based on Markov chain models. Group members compute the group key in a distributed manner. Group key mechanism involves creating and distributing a common secret key among all group members. However, Key management for a large and dynamic group adds to the complexity due to its scalability and security. Modification of any membership value requires the group key to be refreshed to ensure backward and forward secrecy.

Cho (2008; 2010) and Deshpande (2007) adopted a recommendation protocol to exchange, revoke and refresh recommendations about other network entities. By executing a recommendation protocol, the network entity can determine the trust level of the target, while requesting for a certain service. Unfortunately, recommendation-based trust models are very vulnerable to Sybil Attacks. Authors in (Cho, 2010) emphasizes that public-key certificates alone do not assure authentication in MANET, due to the missing reliable central certification.

Garg, K., and Misra (2010) presented a scheme for distributing trust certificates within dynamical mobile wireless ad-hoc networks. The core of the paradigm is offering a method for communication by modifying the environment. The main weakness of this approach is its vulnerability to DOS attacks. Kim et al (2009) proposed an entropy based trust model in which trust is measured as uncertainty. A Trust Model Based Routing Protocol was proposed by Mohamed Salah Bouassida (2007) for Secure Ad Hoc Networks. The trust model uses subjective logic to express trust, but the analysis found that many models fail to manage uncertainty and various weight relationships when a node moves away from other nodes or the node is deficit of evidence. Hence the proposed model is expected to handle dynamic security and manage controlled trust among multiple nodes in a large network.

**Trust analysis and intrusion detection:**

![Fig. 1: Trust based Intrusion Detection system.](image)

Fig. 1 shows Trust based Intrusion detection system SKITE, which works based on node’s traffic intensity. The audit log data of network explains the behavior of node based on its defined trust profile (Saminathan, 2010). A node whose behavior is not as per the expected state has been categorized as vulnerable or considered as an intruder. Ascertaining a node as a trust / untrust node depends on the “recommendation” of nodes which fall within the range. Hence any node, which is identified as neighboring to the requestor node, needs to suggest node with trust value to participate in secured routing process. The requestor node always maintains an update of recommendation metric of its neighbors, before initiating the route to be established.

Many primary factors influence the security impact of MANET nodes during routing process, the most major issues,

(a) New neighboring node entering into the cluster or domain, which may suggest an unsecured forwarding process and hence may hamper the route.
(b) An untrustworthy neighbor node, which does not forward data can be considered as breach of security.
(c) Node with minimal recommendation value, can be considered as unsecured path for session establishment and data transfer.

**Definitions:**

STv follows multiple profiles as node recommendations.

STv adopts the following definitions, where node ‘ni’ belongs Cluster C, where i =\{1, 2, ..., n\}.

(a) Any node ‘ni’ can recommend another node ‘nj’, iff it possesses a Trust Value STv
(b) Any node ‘ni’ can recommend another node ‘nj’, iff it possesses a higher trust value than being recommended.
(c) Node ‘ni’ can update the STv, of recommender node after regular intervals of time or after a process or event is complete.

(d) A node’s recommendation value is dependent on its previous STv (history STV) and neighboring node’s recommendation value.

(e) For any recommendation node ‘ni’, selected as part of cluster Cc, should exchange the security key Ki among other nodes nj, where j=k,l,...,n, such that each node ni \( \not\in \{Cc\} \).

(f) STv path (trusty path) is established, iff all nodes ni belongs to Cc, else another alternate path TPj is selected where ni is subset of Cc.

**Skite polices and definitions:**

SINDER follows trust based recommendation metrics among member nodes which establish communication within a defined cluster. SKITE follows different recommendation metrics in order to understand the node behavior within the domain or cluster. The following recommendation metrics are adopted as shown in Table 1.

<table>
<thead>
<tr>
<th>Recommendation Metric</th>
<th>STv (SKITE Value)</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Trust</td>
<td>9</td>
</tr>
<tr>
<td>Controlled Trust</td>
<td>7</td>
</tr>
<tr>
<td>Acceptable Trust</td>
<td>5</td>
</tr>
<tr>
<td>Moderate Trust</td>
<td>3</td>
</tr>
<tr>
<td>UnTrust</td>
<td>1</td>
</tr>
</tbody>
</table>

Each node updates it neighbor with “recommendation metrics” based on its “instance interval”. Derival of instance interval value is dependent on pervious historic metric earlier adopted and change in metric due to an event on execution (Refer Section-2.1(d)). The recommendation metric value STv, to be referred as SKITE Trust Value maintains the trust value of each node which can be varying from 1 to 9 as shown in Table 1. Node whose STv value greater than and equal to ‘5’ is given priority for security policies and session establishment, while as node whose STv value less than ‘5’ is given lesser priority for session process establishment and may be considered, if and only if there are no other nodes of higher STv value.

![Fig. 2: SKITE Architecture and function.](image)

**Recommendation metrics:**

The trust value STv is being defined unique for each node based on its identity over a time slot ‘ta’. For any given trust relationship between a trusted node in a given trust relationship, there exists multiple relationships among the nodes.

\[
STv = \frac{\sum_{i=0}^{\tau} (NTv[ni]) \times \sum_{j=i} (\rho \cdot ATv[ nj])}{\sum_{i=1}^{n} \{\text{ta}[ni] \times \text{ta}[nj] \}}
\]

Where,

- \( STv = \) SKITE Recommend Trust Value key for node
- \( ni, nj = \) recommender node (in request) and recommendation node
- \( \text{ta} = \) maximum time available for node to maintain trust value
- \( \tau = \) random key value generated from 1 to 5000, to support variable key exchange.
- \( P = \) unique machine identity
NTv = Node Instance Interval value (Refer section 2.1(d))
ATv = Node’s assigned trust value

**Skite – architecture and functionality:**

SKITE architecture (Fig. 2) works on two three modules such as Trust Key Generator, Recommender Node and Security session Manager. Node ‘ni’ requests for trust value STv to Key Generator module (Step-1) which in turn authenticates the node using its unique identity (Step-2). The Recommender Algorithm obtains the trust key (NTv) of the node (Step-3) and assigns the node to Session Manager (Step-4), which in turn generates the asymmetric key (Step-5). The Asymmetric key is exchanged for ATv value obtained from node ‘ni’ (Step-7) and assigned to node ‘ni’ as STv. (Step-6) over the time period ‘ta’.

The assignment of STv among set of nodes within the cluster is shown in Fig. 3. C1 and C2 are clusters of node, where the clustering is carried out based on Hello protocol and neighborhood approach. Algorithm-1 explains the trust value assignment procedure which is adhered based on neighboring node values and instance interval value (NTv).

![Fig. 3: MANET nodes engaging in trust assignment with multiple clusters](image)

When a communication requests happens over AODV-RREQ, then node security STv needs to be verified. Within a cluster the requester node verifies the NTv value of recommender value before a new trust value is to be assigned. As shown in Fig. 3, more than one neighborhood node within Cluster participate in assigning the trust value, hence the summarized STv is assigned based on Equation-1 as discussed in Section 3. A node can assign a positive or negative trust value which is based on session binding and previous security event under negotiation as shown in Table 2. A negative NTv indicates a lesser trust values whose STv is ‘1’ or UnTrust. STv value is returned as “r” for being recommended and “n” for not recommended. STv is generated based on the recommended STv. Each node establishes its contact with another node and updates its distance at consistent time. The beaconing signal strength and adherence to neighbor nodes supports in forming the cluster C.

Algorithm: Recommendation STv
For \( i \in \{1, 2, ..., n\} \)
(1) If NTv exists for a node ‘ni’ then
   STv [ni] = ATv [ni] at time ‘ta’
Else
   Generate STv[ni]
// Verify STv for all nodes on the basis of connectivity
if (ta != 0)
(2) For all nodes [ni] considered as neighbor
HELLO (nj, ATv(ni))
(3) STv_RPLY (ATv(ni)) // uses trust value analysis
(4) For all neighbor node ‘ni’

(a) RPLY \( (ATv[ni], ta) \)

(b) Generate \( STv \) // Equation-1

(c) If \( (\max(STv[ni]) > STv.thresh) \)

++ \( STv.r \) // recommend

Else ++ \( STv.n \) // not recommend

(5) End for

(6) Return \( (STv.x, ta) \)

Until \( (\forall \forall \ \text{neighbor nodes ‘nj’}) \) // updated based on HELLO protocol

If the number of nodes are \( n \) then maximum no of nodes in a graph are \( n(n+1) \). In order to construct the distance matrix for each node, the initially distance value is \( 1/n(n+1) \) as obtained using HELLO protocol. Table 2 shows the \( STv \) assignment matrix among nodes engaged in requesting and responding with recommendation value. The edges denoted in Fig. 4 indicate that there exists a link between the nodes. Each node maintains its own recommended value as well proposes the recommended value to other nodes. The ‘X’ in Table 2 indicates that no value persists for the node, and ‘--’ indicate that no link exists between two or more pair of nodes.

Fig. 4: Recommend Weight Values for nodes.

<table>
<thead>
<tr>
<th>( STv )</th>
<th>A ((0.3))</th>
<th>B ((0.7))</th>
<th>C ((0.6))</th>
<th>D ((-0.9))</th>
<th>E ((0.4))</th>
<th>F ((0.5))</th>
<th>G ((0.5))</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>X</td>
<td>0.30</td>
<td>0.40</td>
<td>0.50</td>
<td>0</td>
<td>---</td>
<td>0.10</td>
</tr>
<tr>
<td>b</td>
<td>0.30</td>
<td>X</td>
<td>0.40</td>
<td>0.50</td>
<td>0.10</td>
<td>---</td>
<td>0.10</td>
</tr>
<tr>
<td>c</td>
<td>0.40</td>
<td>0.40</td>
<td>X</td>
<td>0.40</td>
<td>0.10</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>d</td>
<td>0.50</td>
<td>0.50</td>
<td>0.40</td>
<td>X</td>
<td>1</td>
<td>-0.50</td>
<td>-0.40</td>
</tr>
<tr>
<td>e</td>
<td>0</td>
<td>0.10</td>
<td>0.10</td>
<td>0.10</td>
<td>1</td>
<td>X</td>
<td>0.50</td>
</tr>
<tr>
<td>f</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>-0.50</td>
<td>0.50</td>
<td>X</td>
<td>0</td>
</tr>
<tr>
<td>g</td>
<td>0.10</td>
<td>0.10</td>
<td>---</td>
<td>-0.40</td>
<td>0</td>
<td>0</td>
<td>X</td>
</tr>
</tbody>
</table>

**Experimental test bed:**

The testbed is implemented on MANET nodes varying from 10 to 100 nodes, over a simulation area of 500 mts. Maximum radio range for defining the cluster is set to 250m for identifying the neighbor nodes. To evaluate the proposed SKITE mechanism, ns2 is selected as the simulator to support in trust assignment. The performance parameters of ad-hoc network to support in providing security primarily relate to session management and time taken to establish session. Table 3 shows the testbed parameters, which is executed for simulation time variable set of nodes.

<table>
<thead>
<tr>
<th>Table 3: Simulation testbed parameters.</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Total simulation time</td>
<td>600</td>
</tr>
<tr>
<td>Simulation area</td>
<td>500m*500m</td>
</tr>
<tr>
<td>Total number of nodes</td>
<td>10 to 100</td>
</tr>
<tr>
<td>Radio range</td>
<td>250 m</td>
</tr>
<tr>
<td>Maximum speed</td>
<td>20 m/s</td>
</tr>
<tr>
<td>Pause time</td>
<td>10s</td>
</tr>
<tr>
<td>Data payload</td>
<td>512 bytes</td>
</tr>
<tr>
<td>Traffic Type</td>
<td>CBR</td>
</tr>
<tr>
<td>Type of Attack</td>
<td>Black hole, Worm Hole, Packet Drop Attack</td>
</tr>
<tr>
<td>Maximum connection</td>
<td>10 to 35</td>
</tr>
</tbody>
</table>
The experiment is conducted for multiple sessions with variable CBR services in use. Various types of security attacks are primarily verified such as Worm Hole, Packet Drop attacks and black hole attacks. Dropping of packets due to high latency is a predictable phenomenon in MANET, but dropping of packets by forwarding node indicates vulnerability issues, hence performance of SKITE compared to packet dropping over DSR protocol (Zhan, 2010) is tested using ns2 (Network Simulator, 1989).

Performance analysis:

SKITE performance is analyzed over various metrics related to security approaches in a session. Fig. 5 shows the average number of secured sessions to be managed over variable time interval. It can be found that SKITE shows higher number of secured nodes as time increases compared to PROFIDES, which adapts a trust evaluation technique. The average number of secured nodes is 22.38% higher than SKITE than PROFIDES. Though PROFIDES show a better performance at 40 msecs of test interval, SKITE performs better considerably throughput by maintaining secured sessions.

![Figure 5: Average number of secured sessions managed over time.](image1)

Fig. 6 shows the average latency effect observed for packet drop attack, which shows the performance of SKITE to be at lower rate as on an average to be 32.51% than compared to SAR scheme which performs at an average of 58.69% and ARAN scheme to show an average of 78.93% for 35 mobile nodes. The latency issue primarily due to packet drop rate of vulnerable forwarding node for nodes under session being established.

![Figure 6: Observed Average Latency over presence of malicious nodes for Packet dropping attack.](image2)
The average latency achieved by MANET nodes under mobility for Black Hole attach is shown in Fig. 7. It could be observed that initially the nodes show variable latency issues for all the three approaches of PROFIDES, SKEMA and SKITE, but after the minimal threshold period of ‘ta’ of 20 msecs the nodes converge such that the latency level achieves global minima. The behavior of PROFIDES and SKEMA can be well understood from Fig. 6, Fig. 7 and Fig. 8, where PROFIDES takes more time to converge, hence also the cost involved whereas SKITE takes minimal time to converge, hence lesser the bandwidth used and also overhead cost involved.

**Conclusion and future work:**

SKITE is designed and implemented to provide trust based security mechanism for MANET nodes under dynamic mobility and variable services. Each source node and destination node has to adopt with variable forwarding nodes to transmit and receive the data until completion of session. Hence SKITE is designed such that only nodes with carry the trust value and support in exchange of pair wise keys can participate in data transfer. Such nodes are not vulnerable and hence contribute towards an adaptive secured route mechanism.
SKITE adopts multi-hop trust based secured session management mechanism where node recommendation plays the vital role in selecting a trustworthy node. The combined recommended trust metric value of nodes is considered to approve the node for transmission or disapproves the node. The node is also selected based on their contribution of “Instance Interval Value” and negotiated recommended value and hence key is exchanged. The performance of SKITE is well analyzed over PROFIDES, SKEMA, ARAN and SAR security schemes for variable security attacks. SKITE had well established in terms of time to establish a session, cost overhead, handling attacks and provides high throughput. The future work can be extended to support dynamic trust for different type of mobile nodes based on their service nature and environment.

REFERENCES


